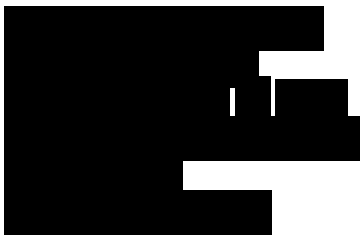
FY 2008 INDEPENDENT AUDIT REPORT ON PRIVACY AND DATA PROTECTION

FEDERAL HOUSING FINANCE BOARD



NOTICE OF SUBSEQUENT EVENTS

On July 30, 2008 and after substantial completion of this audit, the President signed the "Housing and Economic Recovery Act of 2008" (ACT). The Act gives the Finance Board responsibility for winding up the affairs of the Federal Housing Finance Board (FHFB) by July 30, 2009. Consequently, recommendations in this report that relate to matters associated with winding up the affairs of FHFB will be forwarded to the Chairman of FHFB for action under the authorities delegated to him by the Federal Housing Finance Board.

CONTENTS

NOTICE OF SUBSEQUENT EVENTS

On July 30, 2008 and after substantial completion of this audit, the President signed the "Housing and Economic Recovery Act of 2008" (ACT). The Act gives the Finance Board responsibility for winding up the affairs of the Federal Housing Finance Board (FHFB) by July 30, 2009. Consequently, recommendations in this report that relate to matters associated with winding up the affairs of FHFB will be forwarded to the Chairman of FHFB for action under the authorities delegated to him by the Federal Housing Finance Board.

FY 2008 INDEPENDENT AUDIT REPORT ON PRIVACY AND DATA PROTECTION

FEDERAL HOUSING FINANCE BOARD

EXECUTIVE SUMMARY

The Office of Inspector General (OIG), Federal Housing Finance Board (Board) contracted with Cotton & Company LLP to perform a performance audit of privacy and data protection policies and procedures and, specifically, Board compliance with Title V, Section 522, of the Consolidated Appropriations Act of 2005. The Appropriations Act requires agencies to assign a Chief Privacy Officer (CPO) who is responsible for identifying and safeguarding personally identifiable information (PII) and requires an independent third-party review of agency use of PII and of its privacy and data protection policies and procedures at least every two years.

We conducted both the Board's FY2006 and FY2008 privacy audits and noted significant improvements by the Board in developing and implementing privacy and data protection policies, procedures, and practices. While the Board has made significant improvements in their privacy program, we did identify areas where controls can be improved. These issues are discussed in the Summary Results and Detailed Results section of this report. This document discusses engagement objectives, agency background, scope and methodology, and summary and detailed audit results.

Management responses to findings and recommendations in this report were obtained through verbal communications with management. Overall, management agreed with the findings and recommendations contained in this report. Written responses were not obtained due to the planned merger of the Board with the Office of Federal Housing Oversight (OFHEO). OFHEO and the Board are scheduled to merge into the Federal Housing Finance Administration (FHFA) during FY2009 and as early as October 1, 2008. This merger may result in changes to key personnel who would be responsible for responding to findings and recommendations contained in this report.

OBJECTIVES

The Board's OIG contracted with Cotton & Company to conduct a performance audit of the Board's privacy and data protection policies and procedures and compliance with Title V, Section 522, of the 2005 Appropriations Act. Specific audit objectives were to:

- Determine the effectiveness of privacy and data protection policies and procedures. Specifically, determine if Board privacy policies and procedures cover significant areas including but not limited to:
  - Roles and responsibilities of key privacy personnel including Chief Privacy Officer (CPO), Senior Agency Privacy Official (SAPO), and Privacy Officer (PO)
  - Identification of applicable privacy laws and regulations
  - Policies and procedures for complying with applicable privacy laws and regulations
  - Acceptable and unacceptable uses of information in identifiable form
  - Breach notification policies and procedures
  - Intranet and internet privacy policies and procedures
  - Policies and procedures for identifying and safeguarding information in identifiable form
  - Privacy training

- Determine compliance with the Board's stated privacy and data protection policies and applicable regulations, laws, and federal guidance.

- Ensure that all technologies used to collect, use, store, and disclose information in identifiable form allowed for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information.

- Ensure that the Board's description of the use of information in an identifiable form was accurate and accounts for the agency's current technology and its processing of this information.

- Ensure compliance and consistency with online and offline stated privacy and data protection policies.

- Determine if management incorporated analysis of information in identifiable form into its FIPS 199 risk categorization process.

- Analyze FHFB's intranet, network, and websites for privacy vulnerabilities, including noncompliance with stated policies, practices, and procedures and risks for inadvertent release of information in identifiable form from the website.

- Review any prior evaluations or assessments by management of FHFB privacy policies, practices, and procedures, including the FY 2006 Section 522 Privacy Audit Report and FHFB's FY 2007 FISMA submission Section D, Reporting Template for Agency SAOPs.

FEDERAL HOUSING FINANCE BOARD BACKGROUND

The Board is an independent agency established by the Financial Institutions Reform, Recovery, and Enforcement Act of 1989. It is charged with supervising and regulating 12 Federal Home Loan Banks (FHLBanks) and has the statutory duty to ensure that FHLBanks operate in a financially safe and sound manner, are adequately capitalized, and are able to raise funds in the capital markets. The Board also has the statutory duty to ensure that FHLBanks conduct their housing finance mission.

The Board is the successor to the former Federal Home Loan Bank Board, which was established by the Federal Home Loan Bank Act of 1932. The agency's Board of Directors is comprised of five members. Four are appointed by the President and confirmed by the Senate and must have extensive experience or training in housing finance or a commitment to providing specialized housing credit. At least one appointed director must be from an organization with more than a 2-year history of representing consumer protections.

The appointed members of the Board of Directors serve staggered 7-year terms. The President designates the Chair of the Board of Directors from among these appointed members. The fifth member is the Secretary of the Department of Housing and Urban Development. Not more than three directors can be from the same political party.

The Board is a non-appropriated agency that draws its financial resources from assessments on the 12 FHLBanks.

SCOPE AND METHODOLOGY

To accomplish the audit objectives, we assessed the Board's privacy and data security policies, procedures, and practices as of July 25, 2008, for compliance with federal privacy and data security laws and regulations. Specific laws and regulations included in our audit were:

- Title V, Section 522, of the Consolidated Appropriations Act of 2005

- Section 208 of the 2002 E-Government Act (Privacy Provisions)
- 1974 Privacy Act
- Office of Management and Budget Memorandums

We based our audit of the Board's security controls over PII on guidance in the National Institute of Standards and Technology (NIST) Special Publications (SP), Federal Information Processing Standards (FIPS), and Office of Management and Budget memorandums and circulars.

We conducted our audit through detailed interviews, the submission of a privacy questionnaire to all Board employees and contractors, an after-hours walk through of Board office space, and evaluation of Board policies, procedures, and practices.

We conducted interviews to obtain an understanding of the types of information handled by Board personnel and to determine if management had identified and adequately protected PII. We interviewed key persons from senior management, examination staff, Office of the CFO, Office of the CIO, and Office of the General Counsel.

We developed and administered a web-based questionnaire to all Board employees and contractors inquiring about their use of information as part of daily activities and whether any of the information they handled could be considered PII. Based on questionnaire responses, we followed up with additional interviews to determine specifically if PII was being used, processed, stored, or handled by Board personnel.

We conducted an after-hours walk through of the Board's business areas to determine whether sensitive PII in hard copy format was being adequately protected and to determine whether employees and contractors were adequately safeguarding computer passwords and tokens while away from their machines.

The audit included assessing compliance with applicable federal privacy laws and regulations as well as Board policies and procedures related to PII. We reviewed and evaluated all pertinent documentation and privacy impact assessments to determine if privacy and data security considerations were addressed. In addition, where PII was identified, we determined if management was aware that agency personnel had access to PII and if it had implemented adequate controls.

We conducted this performance audit in accordance with Generally Accepted *Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We conducted this audit from May 2008 to July, 2008. We were not requested to, and we cannot, express an opinion as it relates to any financial information or information security controls related to the Board.

Based on audit results, we developed findings and recommendations for management. Summary and detailed findings along with recommendations are below.

SUMMARY RESULTS

Overall, the Board has made significant progress in the development and implementation of privacy and data protection policies, procedures, and practices. Specific progress we noted included the:

- Development and documentation of privacy policies and procedures including specific procedures for responding to the release of PII as required by OMB memorandum M-07-16.
- Development of a social security number and PII reduction plan,
- Submission of the Board's privacy baseline report to the OIG,
- Implementation of two factor authentication on all Board machines, and
- Development and implementation of a privacy training program for employees and contractors.

While the Board did make significant progress with their privacy program we did note a few instances where controls can be strengthened. [redacted]

In addition to the one outstanding [redacted] finding, we noted three new control weaknesses or areas of non-compliance with laws and regulations that support our conclusion and offer recommendations to address these weaknesses.

FY2008 DETAILED RESULTS

1. Privacy Training

Controls were not adequate to ensure all Board employees and contractors received privacy training on an annual basis. Specifically, we conducted audit procedures to determine whether all Board employees and contractors had completed privacy training within the past year. Our review noted six individuals had not completed the required training.

Section 522 (a) of the 2005 Consolidated Appropriations Act (H.R. 4818) states, "Privacy Officer – Each agency shall have a Chief Privacy Officer to assume responsibility for privacy and data protection policy, including (8) training and educating employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies."

In addition, we determined management's process for providing privacy training and identifying and tracking completion does not ensure all individuals with both physical and logical access to FHFB systems and data participate. Specifically, we noted the Board's privacy training is made available online to all employees and contractors with a network account. In addition, management tracks completion of privacy training by comparing a list of all network accounts against a list of individuals who have completed the training. While this process will ensure all individuals with network accounts complete privacy training, it does not address employees or contractors who may not have network accounts for whatever reason.

OMB Memorandum M-08-21 titled "FY2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management", Question 42 "Training" of the Frequently Asked Questions, section states:

> Do employees who never access electronic information systems need annual security and privacy awareness training?

Yes, FISMA and OMB policy (Memorandum M-07-16 Attachment I.A.2.d.) require all employees to receive annual security and privacy awareness training, and they must be included as part of your agency's training totals. When administering your security and privacy awareness training programs, it is important to remember: (i) all employees collect, process, access and/or maintain government information, in some form or format, to successfully perform their duties and support the agency's mission; and (ii) information is processed in various forms and formats, including paper and electronic, and information systems are a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

Without controls in place, which ensure all Board employees and contractors complete privacy training whether or not they have computer access, the risk of sensitive PII being handled in an inappropriate or unsecure manner increases.

Recommendation No. 1

We recommend the CPO:

a. Strengthen controls over the privacy training program to ensure all Board employees and contractors complete privacy training on an annual basis.
b. Develop, document, and implement controls to ensure employees and contractors without network accounts complete privacy training.

2. [redacted]

[redacted]

FY 2008 INDEPENDENT AUDIT REPORT ON PRIVACY AND DATA PROTECTION

[redacted]

Recommendation No. 2

[redacted]

Recommendation No. 3

STATUS OF [redacted] FINDINGS AND RECOMMENDATIONS

Appendix A

Finding	Recommendation	Status
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	
	[redacted]	
	[redacted]	
	[redacted]	
[redacted]	[redacted]	[redacted]

STATUS OF [redacted] FINDINGS AND RECOMMENDATIONS

Finding	Recommendation	Status
[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]

STATUS OF [redacted] FINDINGS AND RECOMMENDATIONS

Finding	Recommendation	Status
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	
	[redacted]	
	[redacted]	
	[redacted]	
	[redacted]	

STATUS OF [redacted] FINDINGS AND RECOMMENDATIONS

Finding	Recommendation	Status
[redacted]	[redacted]	[redacted]

STATUS OF [redacted] FINDINGS AND RECOMMENDATIONS

Finding	Recommendation	Status
[redacted]	[redacted]	
	[redacted]	[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]

[redacted]